Abstract of the Disclosure

A repeatable cryptographic key is generated based on varying parameters which represent physical measurements. Locations within a share table, which locations store valid and invalid cryptographic shares, are identified as a function of received varying parameters. The share table is configured such that locations which are expected to be identified by legitimate access attempts contain valid cryptographic shares, and locations which are not expected to be identified by legitimate access attempts contain invalid cryptographic shares. The share table configuration may be modified based on prior history of legitimate access attempts. In various embodiments, the stored shares may be encrypted or compressed. A keystroke feature authentication embodiment uses the inventive techniques to implement an authentication system which authenticates based on an entered password and the manner in which (e.g. keystroke dynamics) the keystroke is entered. Another embodiment uses the inventive techniques to protect sensitive database information which is accessible using DNA measurements.